

M-12041US
09/940,026REMARKS

Applicants respectfully traverse the lack of written description rejections of claim 1 and 20. For example, consider the limitation recited in claim 1 of "generating a random number at the storage engine and encrypting the random number with a public key extracted from the certificate to form a session key and transmitting the session key to the host." This limitation is plainly supported by Figure 6 and the accompanying description on, for example, page 29, line 13 through page 30, line 2. As shown in Figure 6, the data storage engine (element 604) receives a certificate (element 610) from the host (element 606). After validating the authenticity of the host's certificate, the data storage engine proceeds to generate a random number (in element 618) which will be used as a secure session key (element 620). The generated random number/secure session key is then encrypted with the host's public key extracted from the certificate (element 622) and transmitted back to the host. The accompanying description starting on page 29, line 13 noted above supports Figure 6. For example, Applicants state beginning on line 26 of that page:

In block 614, the host is verified for revocation. Revocation is available at all of the levels of granularity of the certificate as implied by all of the fields. Part of the validation, in one embodiment, requires checking a revocation list 608 on media 602. The engine 604 retrieves the revocation list 608 from the media 602. If the validation process 614 passes at block 616, the engine 604 generates a random number via random number generator 618 to obtain a first portion of a secure session key 620. The engine 604 performs a public key encryption 622 using the first portion of the secure session key 620 and a protocol public key 624 retrieved from the certificate 610. The host 606 receives the encrypted session key, decrypts the encrypted session key at block 626 and produces the secure session key 628. (emphasis added).

In addition, consider the limitation of claim 1 of "receiving an encrypted content key from the storage engine and decrypting the content key using the session key to recover the content key." This limitation is plainly supported by Figure 8 and the accompanying description, for example, on page 40, line 18 through page 41, line 7. As shown in Figure 8, the data storage engine selects a play session key (element 830). The host receives an encrypted version of the play session key (element 832). The host then decrypts the play session key using the session key (element 834). As seen in element 850, the host may then decrypt content using the play

M-12041US
09/940,026

session key. The accompanying description starting on page 40, line 18 supports Figure 8. For example, Applicants state beginning on page 41, line 2 that

After authentication, the engine selects a decryption play session key 830. Block 832 requires delivery of a play session key from the engine to the host, such as a player. A player receives this play session's decryption key for a specified file. Block 834 provides that a host decrypts the play session key using a session key. Block 840 provides that the player receives encrypted content. Block 850 provides that the play session decryption key received at block 832 decrypts the content.

Thus, Applicants respectfully submit that ample written support exists for the amendments previously made to claims 1 and 20.

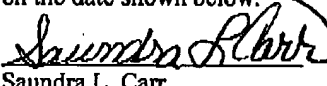
Note the advantages of the method recited in claim 1: the DRM (digital rights management) is controlled by the storage engine rather than a host. This is advantageous because hackers cannot obtain access to the workings of the data storage engine as they would for a typical host such as a PC. In contrast, the Hurtado reference is a conventional "host-based" DRM scheme. There is no suggestion or teaching for the inventive acts of "generating a random number at the storage engine and encrypting the random number with a public key extracted from the certificate to form a session key and transmitting the session key to the host" and "receiving an encrypted content key from the storage engine and decrypting the content key using the session key to recover the content key." Note further that content on the media is encrypted according to a content key. Thus, the host needs the content key to gain access to the content. However, for additional security, the storage engine does not simply provide the content key to the host. Instead, the content key is encrypted using the secure session key. Thus, the host can only recover the content key using the secure session key. As such, the secure session key is not a content key but rather is a key to the content key.

Thus, claim 1 and its dependent claims 2, 5-14, and 16-18 is patentable over the Hurtado reference. Claim 20 is patentable for analogous reasons.


M-12041US
09/940,026CONCLUSION

For the above reasons, claims 1, 2, 5 – 14, 16 – 18, and 20 are now in a condition for allowance. Applicant therefore respectfully requests that a timely Notice of Allowance be issued in this case.

If there are any questions regarding this amendment, the Examiner is invited to call the undersigned at (949) 752-7040.

Certification of Facsimile Transmission	
I hereby certify that this paper is being facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.	
 Sandra L. Carr	July 27, 2005 Date of Signature

Respectfully submitted,


Jonathan W. Hallman
Attorney for Applicants
Reg. No. 42,622
Tel.: (949) 752-7040